Sicherheitskonzept

EasyNotes

|  |  |  |  |
| --- | --- | --- | --- |
| **Datum** | **Version** | **Autor\*in** | **Bemerkung** |
| 20.11.2023 | 1.0 | Andi Tschan | Initialdokument |

Status: Entwurf

Inhaltsverzeichnis

[1. Sicherheitskonzept 2](#__RefHeading___Toc102_1702162029)

[1.1. Verantwortlichkeiten 2](#__RefHeading___Toc104_1702162029)

[1.2. Benutzer-, Rollen- und Zugriffsberechtigungen 2](#__RefHeading___Toc104_1702162029_Copy_1)

[1.3. Netzwerksicherheit 2](#__RefHeading___Toc104_1702162029_Copy_1_)

[1.4. EasyNotes Sicherheitsmassnahmen 2](#__RefHeading___Toc104_1702162029_Copy_11)

[1.4.1. EasyNotes CI 2](#__RefHeading___Toc1199_3736107929)

[1.4.2. Azure Infrastruktur 2](#__RefHeading___Toc1201_3736107929)

[1.4.3. Kubernetes 3](#__RefHeading___Toc1203_3736107929)

[1.4.4. EasyNotes Webanwendung 3](#__RefHeading___Toc1205_3736107929)

# Sicherheitskonzept

Auf Basis dieses Sicherheitskonzeptes müssen für alle relevanten Stellen konkrete Leitlinien entwickelt und herausgegeben werden.

## Verantwortlichkeiten

Die Verantwortlichkeiten müssen so verteilt werden, dass die zuständigen Personen jeweils nur die Verantwortung für ihren Zuständigkeitsbereich tragen müssen.

|  |  |
| --- | --- |
| **Rolle** | **Verantwortlichkeit** |
| Projektleitung | Entwickelt und erlässt Sicherheitsleitlinien und überwacht deren Einhaltung. |
| DevOps-Team | Zuständig für die Einrichtung und Wartung der CI/CD-Pipeline, inklusive Sicherheitsaspekte. |
| Entwicklungsteam | Verantwortlich für die Entwicklung sicherer Codepraktiken und die Einhaltung der Sicherheitsrichtlinien im Entwicklungsprozess. |

## Benutzer-, Rollen- und Zugriffsberechtigungen

Für sämtliche Dienste gilt das Prinzip der minimalen Rechte (Least-Privileg). Für alle Dienste müssen Rollenbasierte Zugriffskontrollen (RBAC) konfiguriert und genutzt werden. Benutzer müssen sich zur Nutzung eines Dienstes authentifizieren und autorisieren lassen.

## Netzwerksicherheit

Sämtliche genutzten Netzwerke müssen segmentiert und mit dem Einsatz von Firewalls geschützt werden. Es sollen jeweils nur diejenigen Protokolle und Dienste verfügbar sein welche auch effektiv im Einsatz sind.

## EasyNotes Sicherheitsmassnahmen

### EasyNotes CI

|  |  |
| --- | --- |
| **Massnahme** | **Bemerkungen** |
| Zugriff auf das GitLab Projekt für die Entwickler\*innen wird über SSH Private/Public Schlüssel gesteuert. |  |
| Zugriff auf die GitLab-Container-Registry wird über Access-Tokens gesteuert. |  |
| Den Entwickler\*innen ist es untersagt die .gitlab-ci.yml zu verändern. |  |
| Es dürfen keine vertraulichen Informationen wie z.B. Usernamen, Passwörter oder Acces-Token in der Pipeline enthalten sein. |  |

### Azure Infrastruktur

|  |  |
| --- | --- |
| **Massnahme** | **Bemerkungen** |
| Nur das Dev/Ops Team hat Zugriff auf die Azure Infrastruktur. |  |
| Der Zugriff auf die einzelnen Services müssen mit RBAC umgesetzt werden. |  |
| Nur die benötigten Ports dürfen gegen Aussen offen sein. |  |
| Es müssen Netzwerksicherheitsgruppen verwendet werden. |  |

### Kubernetes

|  |  |
| --- | --- |
| **Massnahme** | **Bemerkungen** |
| Der Zugriff auf den Kubernetes-Cluster soll nur über eine gesicherte Verbindung möglich sein. |  |
| Für die Anwendung EasyNotes ist ein eigener Namespace zu verwenden. Personen mit Zugang zu EasyNotes sollen nur Zugang zu diesem Namespace haben. |  |
| Es sollen keine nativen Kubernetes-Secrets verwendet werden. Stattdessen muss der Azure Key Vault verwendet werden. |  |
| Es müssen Netzwerksicherheitsgruppen verwendet werden. |  |
| Der Zugang zum GitOps-Repository mit der Kubernetes-Konfiguration für EasyNotes muss kontrolliert werden |  |

### EasyNotes Webanwendung

|  |  |
| --- | --- |
| **Massnahme** | **Bemerkungen** |
| Die Webanwendung muss über eine gesicherte Verbindung mit TLS geschützt sein. |  |